Ründepuud

Aivo Jürgenson

Elioni Ettevõtted AS

Tallinna Tehnikaülikool

9th December 2008

Riskide modelleerimine

Eesmärk

- Analüüsida ja esitada keeruliste rünnete struktuuri.
- Leida kõige ökonoomsem rünne.
- Põhjendada turvameetmete vajalikkus.
- Rakendada turvameetmeid kõige mõistlikumas kohas.

Ajalugu

- 1981 — Fault Tree Handbook — US Nuclear Regulatory Comission

Ajalugu

- 1981 — Fault Tree Handbook — US Nuclear Regulatory Comission
- 1991 — A System security engineering process — J. D. Weiss

Ajalugu

- 1981 — Fault Tree Handbook — US Nuclear Regulatory Comission
- 1991 — A System security engineering process — J. D. Weiss
- 1999 — Attack trees: Modeling security threats — Bruce Schneier

Ajalugu

- 1981 — Fault Tree Handbook — US Nuclear Regulatory Comission
- 1991 — A System security engineering process — J. D. Weiss
- 1999 — Attack trees: Modeling security threats — Bruce Schneier
- 2006 — Rational Choice of Security Measures via Multi-Parameter Attack Trees — Ahto Buldas, Peeter Laud, Jaan Priisalu, Märt Saarepera, Jan Willemson.

Ajalugu

- 1981 — Fault Tree Handbook — US Nuclear Regulatory Comission
- 1991 — A System security engineering process — J. D. Weiss
- 1999 — Attack trees: Modeling security threats — Bruce Schneier
- 2006 — Rational Choice of Security Measures via Multi-Parameter Attack Trees — Ahto Buldas, Peeter Laud, Jaan Priisalu, Märt Saarepera, Jan Willemson.
- 2008 — Computing exact outcomes of multi-parameter attack trees — Aivo Jürgenson, Jan Willemson

Ründe struktuur

- Ründaja eesmärk on puu juureks.
- Puu sõlmedeks on AND või OR sõlmed.
- Puu lehtedeks on elementaarründed.
- Puu lehe väärtuseks on üks parameeter.
  - Võimalikkus, spetsiaalsete vahendite vajalikkus, oskuste olemasolu, maksumus, jms.

Mäng

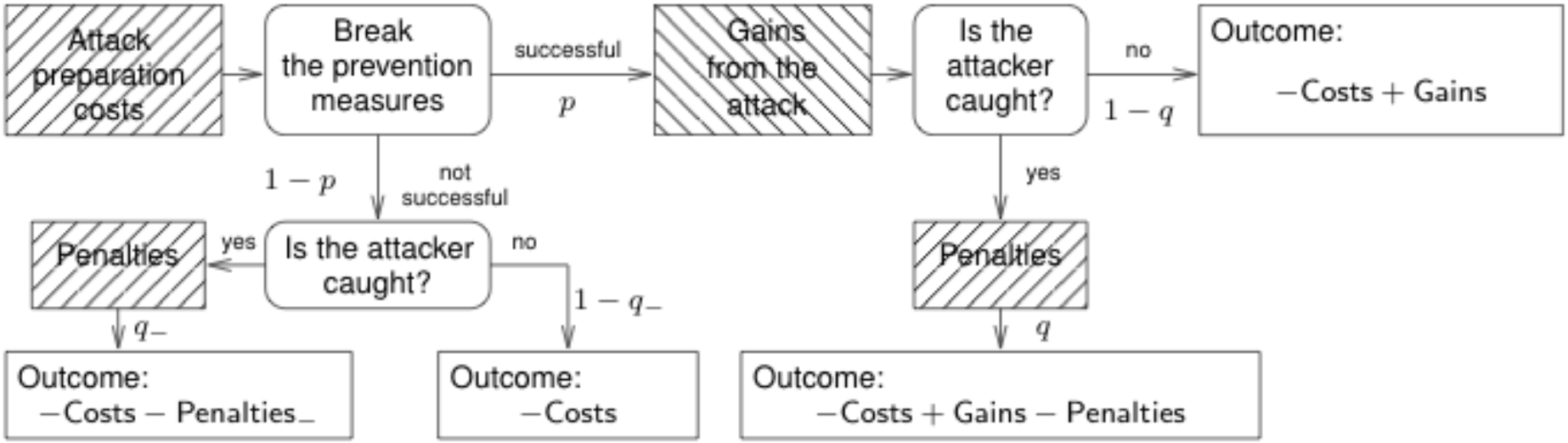


Fig. 2. Diagram (event tree) of the "attack game" from the attacker's point of view

Parameetrid

Parameeter	Tähis
Ründe tulu	Gains
Ründe maksumus	Cost
Ründe õnnestumise tõenäosus	p
Trahv vahelejäämisel, rünne õnnestus	$\pi^+ = q^+ \cdot \mathrm{Penalties}^+$
Trahv vahelejäämisel, rünne ebaõnnestus	$\pi^- = q^- \cdot \mathrm{Penalties}^-$
Ründe kasum	Outcome

Arvutusvalemid

OR:

$$(\mathrm{Cost}, p, \pi^+, \pi^-) = \begin{cases} (\mathrm{Cost}_1, p_1, \pi_1^+, \pi_1^-), & \text{if } \mathrm{Outcome}_1 > \mathrm{Outcome}_2 \\ (\mathrm{Cost}_2, p_2, \pi_2^+, \pi_2^-), & \text{if } \mathrm{Outcome}_1 \leq \mathrm{Outcome}_2 \end{cases}$$

Tulusus:

$$\mathrm{Outcome}_i = p_i \cdot \mathrm{Gains} - \mathrm{Cost}_i - p_i \cdot \pi_i^+ - (1 - p_i) \cdot \pi_i^- .$$

AND:

$$\begin{aligned} \mathrm{Costs} &= \mathrm{Costs}_1 + \mathrm{Costs}_2, \quad p = p_1 \cdot p_2, \quad \pi^+ = \pi_1^+ + \pi_2^+, \\ \pi^- &= \frac{p_1(1-p_2)(\pi_1^+ + \pi_2^-) + (1-p_1)p_2(\pi_1^- + \pi_2^+)}{1 - p_1 p_2} + \\ &\quad + \frac{(1-p_1)(1-p_2)(\pi_1^- + \pi_2^-)}{1 - p_1 p_2} \ . \end{aligned}$$

Senise mudeli vead (1)

- Ekvivalentsed puud annavad erinevad tulemuse
- $T_1 = A \vee (B \& C)$
- $T_2 = (A \vee B) \& (A \vee C)$
- Gains $= 10000$
- $p_A = 0.1$, $p_B = 0.5$, $p_C = 0.4$
- $\text{Expenses}_A = 1000$, $\text{Expenses}_B = 1500$, $\text{Expenses}_C = 1000$
- $\text{Outcome}_{T_1} = 0$
- $\text{Outcome}_{T_2} = -500$

Senise mudeli vead (2)

- Ei leita parimat ründekomplekti:
- $T = (A \vee B)\&C$
- Gain $= 10000$
- $p = 0.8$, Cost $= 100$, $\pi^+ = 1000$, $\pi^- = 1000$

Ründekomplektid

- *attack tree* – ründepuu, Boole valem
  - $\mathcal{F} = (A \vee B)\&C$
- *attack suite* – ründekomplekt, elementaarrünnete hulk
  - $\sigma_1 = A; \sigma = B; \sigma_3 = C; \sigma_4 = A, B; \ldots$
- *satisfying attack suite - rünnet realiseeriv ründekomplekt*
  - $\mathcal{F}(\sigma := \text{true}) = \text{true}$
- ründekomplekti õnnestumise tõenäosus
  - p_σ
- ründekomplekti kulud
  - $\sum_{X_i \in \sigma} \text{Expenses}_i$

Arvutusvalemid

Arvutusvalemid

$$\mathsf{Outcome} = \max\{\mathsf{Outcome}_\sigma : \sigma \subseteq \mathcal{X},\, \mathcal{F}(\sigma := \mathsf{true}) = \mathsf{true}\}\,. \qquad (1)$$

Arvutusvalemid

$$\mathrm{Outcome} = \max\{\mathrm{Outcome}_\sigma : \sigma \subseteq \mathcal{X},\, \mathcal{F}(\sigma := \mathrm{true}) = \mathrm{true}\}\,. \tag{1}$$

$$\mathrm{Outcome}_\sigma = p_\sigma \cdot \mathrm{Gains} - \sum_{X_i \in \sigma} \mathrm{Expenses}_i\,, \tag{2}$$

Arvutusvalemid

$$\text{Outcome} = \max\{\text{Outcome}_\sigma : \sigma \subseteq \mathcal{X},\, \mathcal{F}(\sigma := \text{true}) = \text{true}\}\,. \tag{1}$$

$$\text{Outcome}_\sigma = p_\sigma \cdot \text{Gains} - \sum_{X_i \in \sigma} \text{Expenses}_i\,, \tag{2}$$

$$p_\sigma = \sum_{\substack{\rho \subseteq \sigma \\ \mathcal{F}(\rho:=\text{true})=\text{true}}} \prod_{X_i \in \rho} p_i \prod_{X_j \in \sigma \setminus \rho} (1 - p_j)\,. \tag{3}$$

Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$

Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$

- $\sigma_1 = \{A, C\}, \sigma_2 = \{B, C\}, \sigma_3 = \{A, B, C\}$

Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$
- $\sigma_1 = \{A, C\}, \sigma_2 = \{B, C\}, \sigma_3 = \{A, B, C\}$
- $\text{Outcome}_{\sigma_1} = \text{Outcome}_{\sigma_2} = 4200$

Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$
- $\sigma_1 = \{A, C\}, \sigma_2 = \{B, C\}, \sigma_3 = \{A, B, C\}$
- $\text{Outcome}_{\sigma_1} = \text{Outcome}_{\sigma_2} = 4200$
- $\rho_1 = \{A, C\},\ \rho_2 = \{B, C\},\ \rho_3 = \{A, B, C\}$

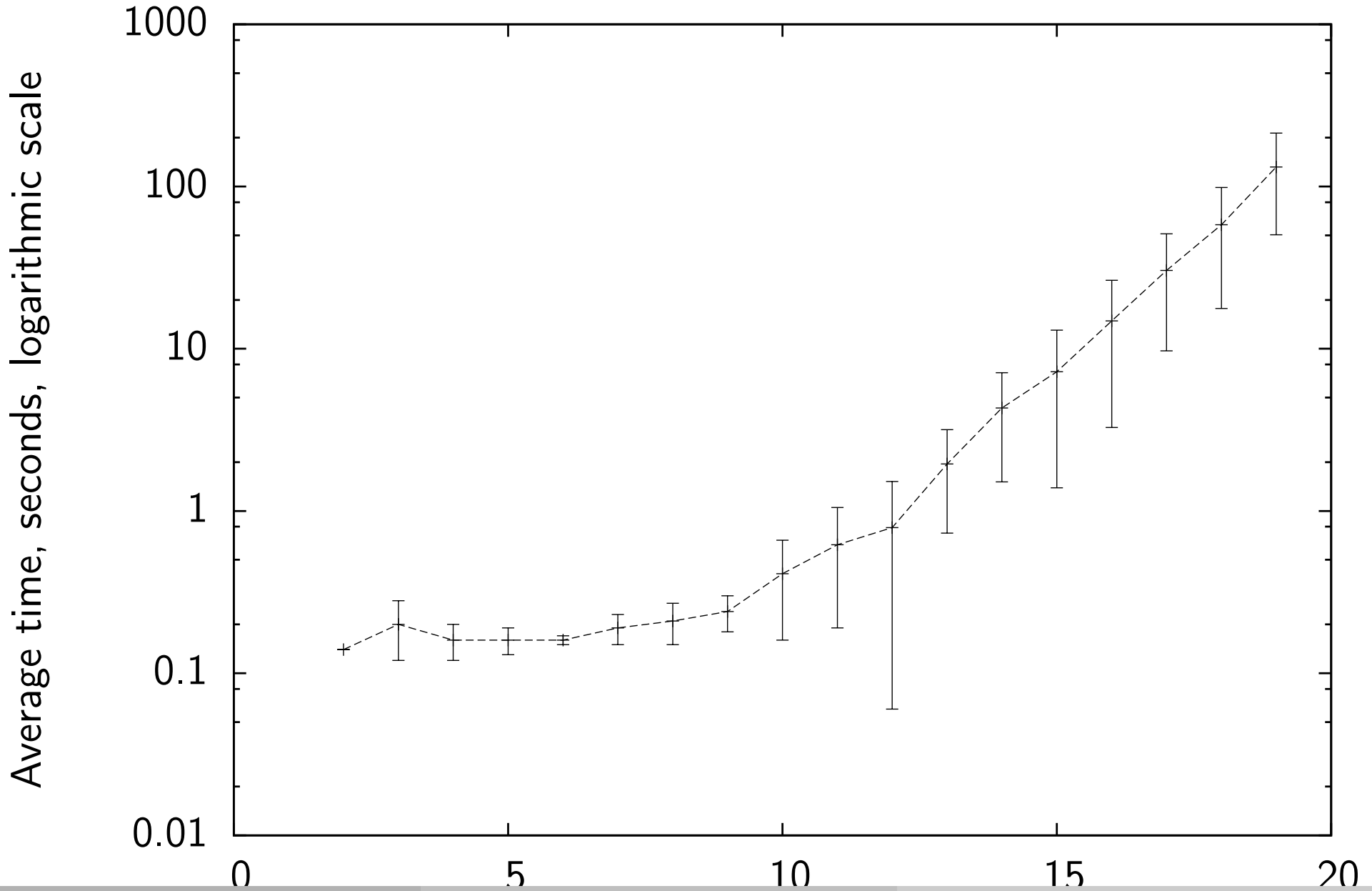
Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$
- $\sigma_1 = \{A, C\}, \sigma_2 = \{B, C\}, \sigma_3 = \{A, B, C\}$
- $\text{Outcome}_{\sigma_1} = \text{Outcome}_{\sigma_2} = 4200$
- $\rho_1 = \{A, C\},\ \rho_2 = \{B, C\},\ \rho_3 = \{A, B, C\}$
- $p_{\sigma_3} = p_A p_B p_C + p_A p_C (1 - p_B) + p_B p_C (1 - p_A) = 0.768$

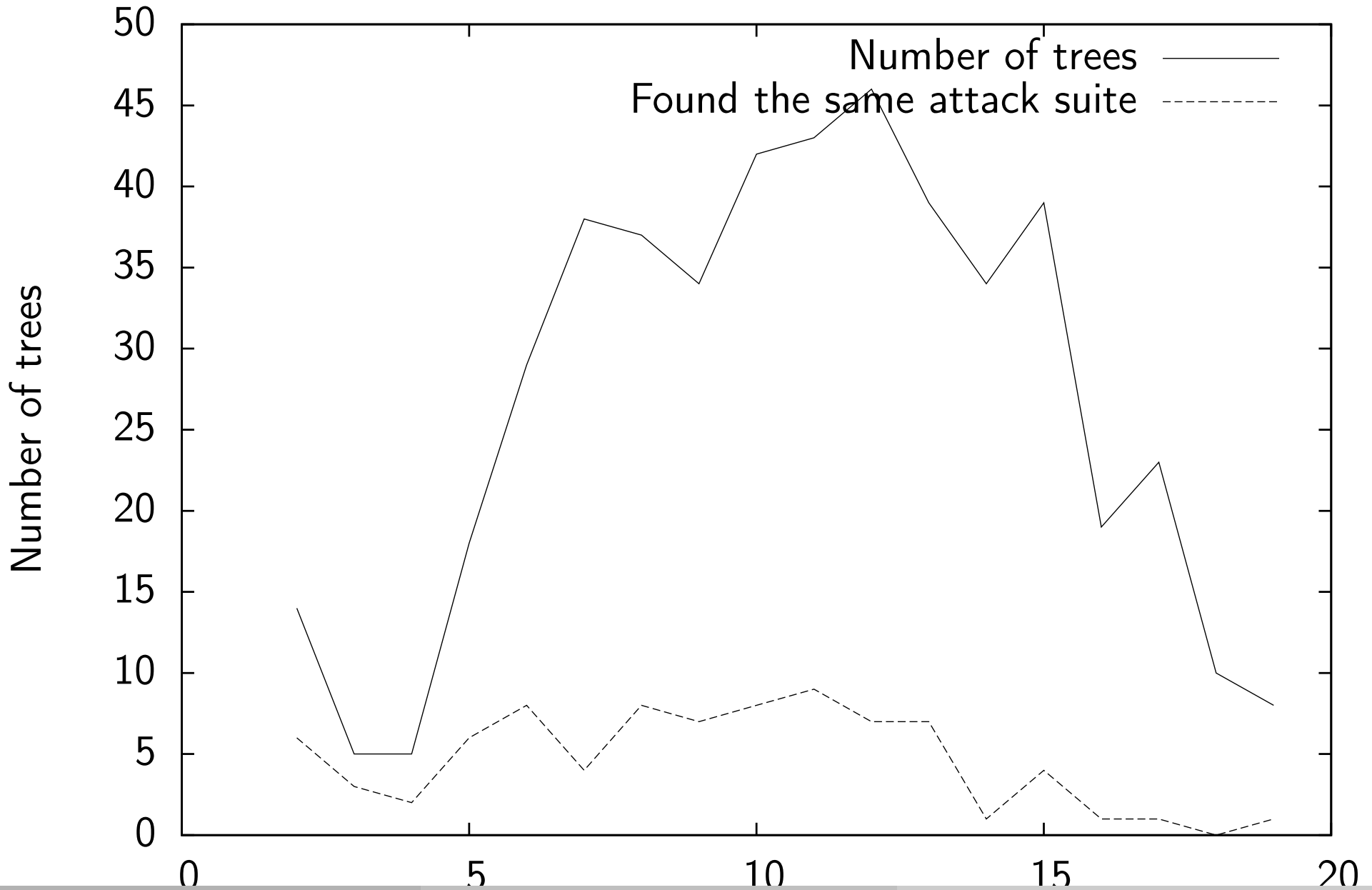
Arvutusnäide

- $T = (A \vee B)\&C$
- Gain $= 10000$
- Expenses $= 1100$
- $\sigma_1 = \{A, C\}, \sigma_2 = \{B, C\}, \sigma_3 = \{A, B, C\}$
- $\text{Outcome}_{\sigma_1} = \text{Outcome}_{\sigma_2} = 4200$
- $\rho_1 = \{A, C\},\ \rho_2 = \{B, C\},\ \rho_3 = \{A, B, C\}$
- $p_{\sigma_3} = p_A p_B p_C + p_A p_C (1 - p_B) + p_B p_C (1 - p_A) = 0.768$
- $\text{Outcome}_{\sigma_3} = \text{Outcome}_T = 4380$

Jõudlus


Average time, seconds, logarithmic scale
1000
100
10
1
0.1
0.01
0
5
10
15
20

Täpsus


Number of trees
Found the same attack suite
Number of trees
0
5
10
15
20
25
30
35
40
45
50
0
5
10
15
20

Kokkuvõte

- Ründepuudega saab edukalt analüüsida keerulisi ründeid.
- Olemasoleva mudelite piiranguid arvestades saab analüüsida ka rünnete kasumlikkust.
- Võib teha Excelis, võib kirjutada enda tarkvara, võib osta paketi
  - www.isograph-software.com - AttackTree+
  - www.amenaza.com - SecurITree
- Microsoft kasutab ründepuude metoodikat SDL (Security Development Lifecycle) raamistikus
  - Threat Modelling Tool